REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

I. OBJECTIONS TO THE SPECIFICATION

The Examiner objects to the Abstract of the present application because the Abstract allegedly exceeds the 150-word limit. However, the Applicants respectfully submit that the Abstract contains only 144 words and therefore adheres to the proper format. Accordingly, the Applicants respectfully request that the objection to the Abstract be withdrawn.

II. REJECTION OF CLAIMS 1, 2 AND 4 UNDER 35 U.S.C. § 102

Claims 1, 2 and 4 stand rejected as being anticipated by the Hoseit et al. patent (U.S. 5,475,365, hereinafter "Hoseit"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Hoseit fails to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claims 1 and 4. Specifically, Applicants' claims 1 and 4 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state; and

(b) adjusting a prior belief state of the first sensor, the adjustment based at least in part on the second sensor's belief state. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a monitored resource; and

(b) adjusting a prior belief state of the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm. (Emphasis added)

Nowhere does Hoseit teach or even suggest the desirability of adjusting a belief state of a sensor, based on a belief state of another sensor. As described in the Applicants' specification, a first sensor in an intrusion detection system may maintain a belief state reflecting a current observation that indicates some system condition or state. By transmitting a second sensor's belief state (which may be based on a different observation) to the first sensor, the first sensor's belief state may be adjusted to increase the overall sensitivity of the intrusion detection system and to reduce false alarms (*See*, for example, page 5, lines 11-15). For example, a first sensor that observes network resources may detect that a server is malfunctioning. This belief state may be transmitted to a second sensor that observes network traffic, and the second sensor may then modify its belief state so that normal network traffic directed toward the malfunctioning server does not trigger a false alarm.

The portions of Hoseit that the Examiner cites as allegedly teaching this limitation in fact only teach that two individual sensors each send some signal to a system monitoring or control unit, which then determines, based on the timing of the individual signals, whether an intrusion has occurred. This is not the same as adjusting a belief state of a sensor; nowhere does Hoseit teach, anticipate or suggest that a sensor can be modified in any manner. Hoseit thus fails to teach or anticipate a method in which a first sensor's belief state is adjusted based on at least part of a second sensor's belief state, as positively claimed by the Applicants in claims 1 and 4. Therefore, the Applicants submit that independent claims 1 and 4 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Hoseit. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

III. REJECTION OF CLAIM 5 UNDER 35 U.S.C. § 102

Claim 5 stands rejected as being anticipated by the Harrison patent (U.S. 5,517,429, hereinafter "Harrison"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Harrison fails to disclose or suggest the novel invention adjusting a belief state of a first sensor based on a belief state of a second sensor regarding the existence or validity of services supported on monitored computer system resources, as claimed in Applicants' independent claim 5. Specifically, Applicants' claim 5, positively recites:

> 5. A method for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:
> (a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources; and
> (b) adjusting a prior belief state of the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious. (Emphasis added)

Nowhere does Harrison teach or even suggest the desirability of modifying a sensor in any way, and Harrison specifically does not teach or suggest adjusting a belief state of a sensor, based on a belief state of another sensor, as positively recited in Applicants' claim 5. The portions of Harrison that the Examiner cites as allegedly teaching this limitation in fact only teach that a plurality of individual sensors each send some signal to a neural network computer (a central controller unit) that processes the individual signals in order to produce a virtual model of a monitored physical space. This is not the same as adjusting a belief state of a sensor. Harrison thus fails to teach

or make obvious a method in which a first sensor's belief state is adjusted based a second sensor's belief state regarding the existence or validity of services supported on monitored computer system resources, as positively claimed by the Applicants in claim 5. Therefore, the Applicants submit that independent claim 5 fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

IV. REJECTION OF CLAIMS 6-9 UNDER 35 U.S.C. § 102

Claims 6-9 stand rejected as being anticipated by the Noorhosseini et al. patent (U.S. 6,707,795, hereinafter "Noorhosseini"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Noorhosseini fails to disclose or suggest the novel invention of adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match, as claimed in Applicants' independent claims 6, 7 and 9. Specifically, Applicants' claims 6, 7 and 9 positively recite:

6. A method for organizing alters into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;

(b) comparing the new alert to one or more existing alert classes;

(c) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(d1) associating the new alert with the existing alert class that the new alert most closely matches; or

(d2) defining a new alert class that is associated with the new alert. (Emphasis added)

7. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a similarity expectation for one or more feature values;

(d) comparing the new alert with one or more alert classes, and either:
(e1) associating the new alert with the existing alert class that the new alert most closely matches; or
(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

9. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:
(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding features;
(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
(c) comparing the new alert to one or more alert classes;
(d) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
(e1) associating the new alert with the existing alert class that the new alert most closely matches; or
(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

Nowhere does Noorhosseini teach or even suggest the desirability of adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match. As described in the Applicants' specification, the nature of an alert may affect a similarity expectation that indicates which features (*e.g.*, source IP address, destination IP address, type of attack, etc.) of the alert should be similar to corresponding features of an existing alert class (*See*, for example, page 6, lines 15-18 and page 7, line 13 – page 9, line 11). For example, if a new alert indicates a SYN flood attack (in which source IP addresses are typically forged), similarity of source IP addresses might not provide a meaningful basis for comparison between the new alert and an existing alert class. Thus, when comparing the new alert to an existing alert class for correlation purposes, it may be necessary to adjust or update this similarity expectation in order to make a meaningful comparison.

The portions of Noorhosseini that the Examiner cites as allegedly teaching this limitation in fact only teach an inference engine that generally executes rules for processing alarms based on whether an alarm is a root-cause alarm or a symptomatic alarm. This is not the same as adjusting or updating a similarity expectation for features

values of a new alert and an existing alert class. Noorhosseini thus fails to teach or make obvious a method for organizing alerts in which an expectation that feature values of a new alert and feature values of an existing alert class will match is adjusted or updated, as positively claimed by the Applicants in claims 6, 7 and 9. Therefore, the Applicants submit that independent claims 6, 7 and 9 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 8 depends from claim 7 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 8 is not anticipated by the teachings of Noorhosseini. Therefore, the Applicants submit that dependent claim 8 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

V. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Hoseit in view of the Timm patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Hoseit and Timm, singularly or in any permissible combination, fail to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above.

As discussed above,nowhere does Hoseit teach or even suggest the desirability of adjusting a belief state of a sensor, based on a belief state of another sensor. Timm does not bridge this gap in the teachings of Hoseit. Hoseit and Timm, singularly or in any permissible combination, thus fail to teach or make obvious a method in which a first sensor's belief state is adjusted based on at least part of a second sensor's belief state, as positively claimed by the Applicants in claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Hoseit in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

10/26/04
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Moser, Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702